REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
09-09-2010	Final Report	1-Sep-2006 - 31-Aug-2010

4. TITLE AND SUBTITLE
Final report

5a. CONTRACT NUMBER
W911NF-06-1-0424

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS
F. Fekri, E. Ayday, R. Subramanian

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Georgia Tech Research Corporation
Office of Sponsored Programs
505 10th Street, N.W.
Atlanta, GA 30332 -0415

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
49586-CS.21

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
This report summarizes the achievements at Georgia Institute of Technology in securing wireless sensor networks funded by the Army Research Office (ARO) during the period of August 1, 2006 to August 31, 2010. The primary goal of the entire research has been to develop techniques that will enable symmetric key cryptography in

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Faramarz Fekri
UU	UU	UU	UU		19b. TELEPHONE NUMBER 404-894-3335

Report Title

Final report

ABSTRACT

This report summarizes the achievements at Georgia Institute of Technology in securing wireless sensor networks funded by the Army Research Office (ARO) during the period of August 1, 2006 to August 31, 2010. The primary goal of the entire research has been to develop techniques that will enable symmetric key cryptography in wireless sensor networks. Key pre-distribution, where some key information is placed in the nodes prior to sensor-node deployment, is advocated to be the most suitable solution for sensor networks. The goal of this research has been to introduce new key pre-distribution schemes and analyze the interplay of the many properties of the random key management schemes and networking of sensors jointly. Furthermore, the research investigates the impact of adversary attacks on the network properties (e.g., required communication radius for connectivity, latency, throughput, average path length, etc.) when key pre-distribution is employed.

List of papers submitted or published that acknowledge ARO support during this reporting period. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

E. Ayday, F. Delgosha, and F. Fekri, "Data Authenticity and Availability in Multi-hop Wireless Sensor Networks," ACM Transactions on Sensor Networks, accepted Jan. 2010.

Number of Papers published in peer-reviewed journals: 1.00

(b) Papers published in non-peer-reviewed journals or in conference proceedings (N/A for none)

Number of Papers published in non peer-reviewed journals: 0.00

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts): 0

Peer-Reviewed Conference Proceeding publications (other than abstracts):

E. Ayday, H Lee, and F. Fekri, "Trust Management and Adversary Detection for Delay Tolerant Networks," Proc. Military Communication Conference, MILCOM 2010, San Jose, CA, Oct. 2010.

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts): 1

(d) Manuscripts

1. E. Ayday and F. Fekri, "A secure multihop broadcasting scheme to provide availability, reliability and authentication for ad-hoc wireless networks," submitted to ACM Transactions on Sensor Networks}, submitted Jan. 2010.

2. R. Subramanian and F. Fekri, "Modeling and Analysis of Latency in Distributed Sensor Networks for Converge-cast Traffic," ACM Transactions on Sensor Networks, submitted in Sept. 2010.

Number of Manuscripts: 2.00

Patents Submitted

Patents Awarded

Graduate Students

NAME	PERCENT_SUPPORTED
Erman Ayday	0.90
Ramanan Subramanian	0.25
A. Beirami	0.05
FTE Equivalent:	**1.20**
Total Number:	**3**

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Faramarz Fekri	0.16	No
FTE Equivalent:	**0.16**	
Total Number:	**1**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period:	0.00
The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:.....	0.00
The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:.....	0.00
Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):	0.00
Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:	0.00
The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense	0.00
The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:	0.00

Names of Personnel receiving masters degrees

NAME

Total Number:

Names of personnel receiving PHDs

NAME
Ramanan Subramanian

Total Number: 1

Names of other research staff

NAME PERCENT_SUPPORTED

FTE Equivalent:

Total Number:

Sub Contractors (DD882)

Inventions (DD882)

Final Performance Report to the

Army Research Office (ARO)

Grant Number: 49586-CI

Design Principles for Secure Wireless Sensor Networks: Key Management Schemes and Malicious Attacks

Georgia Institute of Technology

Principal Investigator:

Faramarz Fekri

School of Electrical and Computer Engineering
Georgia Institute of Technology
Atlanta, Georgia 30332-0250
Email: fekri@ece.gatech.edu
Phone: 404-894-3335
Fax: 404-894-8363

Time Period Covered: August 1, 2006- August 31, 2010

1 Introduction and Research Accomplishments

This report summarizes the achievements at Georgia Institute of Technology in securing wireless sensor networks funded by the Army Research Office (ARO) during the period of August 1, 2006 to August 31, 2010. The primary goal of the entire research has been to develop techniques that will enable symmetric key cryptography in wireless sensor networks. Key pre-distribution, where some key information is placed in the nodes prior to sensor-node deployment, is advocated to be the most suitable solution for sensor networks. The goal of this research has been to introduce new key pre-distribution schemes and analyze the interplay of the many properties of the random key management schemes and networking of sensors jointly. Furthermore, the research investigates the impact of adversary attacks on the network properties (e.g., required communication radius for connectivity, latency, throughput, average path length, etc.) when key pre-distribution is employed.

In the first report (2006-2007), we motivated the research by arguing that existing work on key pre-distribution schemes [1, 2, 3, 4, 5], have several shortcomings: 1. The key pre-distribution parameters were designed independent of the attack models (e.g., node spoofing was not considered by the existing work), 2. Previous work assumes an infinite communication radius for sensor nodes (i.e., the required communication radius for secure connectivity for a network under attack cannot be obtained by the past work in the key pre-distribution schemes), 3. The effect of key pre-distribution on the properties of interest in sensor networks (e.g., latency, throughput, etc.) has not been analyzed by the existing work, and 4. The past work does not consider how the network properties such as latency, throughput, and connectivity would change under adversary attacks. To achieve the above mentioned goals, the primary focus in the first period (August 2006 through July 2007) was 1. to develop a new key pre-distribution method based on symmetric polynomials (which we called MKPS), 2. to analyze the secure link properties of the proposed key distribution scheme under attacks, 3. to extend the proposed key pre-distribution technique to the case where prior information about node locations is available and 4. to develop preliminary results on the relationship between the required communication radius for global network connectivity and node compromise attacks for any general key pre-distribution schemes.

In the second period of the work (covering the work performed from August 2007 through July 2008), we achieved two main objectives. 1. We developed an algorithm to find the optimal dimension in our MKPS scheme, resulting some relatively surprising results that provided new insights on the design of key pre-distribution schemes and introduced new ways we may address security challenges in distributed sensor networks. Specifically, we showed that security can be improved by using the giant component of the network. 2. We developed a geometric model for a randomly deployed sensor network that realistically models dependency of the required communication radius (for global network connectivity) on both key distribution parameters and node compromise attacks. Using this model, we can study as to how the key distribution parameters affects the required sensor communication radius for having connectivity in different key pre-distribution schemes. The proposed model

also facilitated to determine the communication range requirements for providing secure connectivity to a network as a function of the fraction of compromised nodes; for various choices of the key pre-distribution schemes.

In the third period of the work (covering the work performed from August 2008 through July 2009), we accomplish the following main tasks of the project objectives: 1 We addressed the problem of modeling latency and throughput in a convergecast (i.e., data-gathering scenario) wireless sensor network that is secured using a host of key predistribution schemes. Then, we investigated the interplay of key pre-distribution parameters of our proposed MKPS scheme with network properties (e.g, latency, throughput) with and without malicious attacks and compared them with those of the other key pre-distribution schemes. In a typical sensor-network application, reliability and efficiency are of paramount importance. The performance of a network is adversely affected by the compromise of its security, in whole or in part, as compromised nodes and communication links are rendered unusable. It is also necessary for the performance of these networks to not sharply degrade as a result of any security measures implemented in the network. Specifically, the average delay incurred in delivering a message to the sink node, called the *latency*, is a critical performance measure in applications such as military surveillance, chemical hazard detection etc. Hence, it is valuable to analyze and understand the effects adversary attack on latency in a secure sensor network, in which sensor devices may also employ periodic sleep-active duty-cycling to conserve precious energy. We provided a comprehensive approach leading to analytical formulations which enables one to reliably estimate the latency and throughput capacity of secure wireless sensor networks as a function of its security parameters, such as the key-predistribution and attack-model parameters. 2. We investigated temporal aspects of networking to enable the measurement of average packet latency and maximum achievable throughput. We considered two key predistribution schemes and wireless sensor networks and examined the resilience of latency and throughput as a function of node compromise attacks. We compared our proposed key predistribution (MKPS) with the QCOMP scheme. We concluded that MKPS possesses superior resilience with respect to average packet latency and maximum achievable throughput in the presence of adversary. Further, we have analyzed packet latencies with respect to their distance from the sink node. We obtained similar results when comparing MKPS and QCOMP in this scenario as well. Furthermore, we noted that as the dimension of the hypercube in MKPS scheme increases, the resilience of the network to node-compromise attacks improves with the cost of an increased average packet latency.

Finally, in the last year of the work (covering the work performed from August 2009 through August 2010), we achieved the following main objectives. We investigated analytically and experimentally node-spoofing attacks on the key predistribution schemes for wireless sensor networks. Then we designed new key predistribution schemes that resist node spoofing. Current key predistribution schemes for wireless sensor networks derive the merit of their performance based on the resilience of secure communication links to node-compromise attacks without regard to the node spoofing. However, node spoofing can be considered one of the most threatening attacks that can have devastating effect on the net-

work security. Unfortunately, random key predistribution schemes, by their design nature, are very prone to these attacks. As an adversarial entity gathers key information, it is able to mount attacks by spoofing or eavesdropping on networked communications with growing success. A powerful variety of attack is possible with a spoofed node, which is when the adversary is able to present itself as a legitimate identity in the network and not be detected. In this work, we considered the security of wireless sensor networks with a priority on node-spoofing attacks, which was lacking in all the previous random key predistribution schemes. We proposed node-spoofing attack models to classify various adversarial capabilities. Specifically, we proposed two knowledge models for the adversary with regard to node-spoofing attacks, namely, random attack and optimized attack. The idea of the mote-class attacker and the laptop-class attacker are considered with these knowledge models for the node spoofing attack. In the random attack, the mote-class attacker does not have knowledge of node locations or deployment topology. Therefore, this attacker is only capable of randomly compromising nodes throughout the network. For each successive node capture, the adversary selects a node at random. In the optimized attack, we considered a more capable adversary - the laptop-class attacker. This attacker have a global understanding of the topology of the network along with the location and identities of all deployed nodes. The adversary optimizes the node-spoofing attack by maximizing the total number of keys removed from the nodes in the network. This is done by optimizing the set of nodes that the adversary captures. We examined the node-spoofing attack on key predistribution schemes. Additionally, we proposed two new key predistribution schemes that provide a higher resilience to the node-spoofing attack: regular key predistribution (REG) and threshold regular KPS (TKEY). Both of these schemes provide an increased resilience to the node-spoofing attack in the lower range of the probability of establishing a secure link, where link security is high. The gains are realized by enforcing a uniform distribution of keys present in the nodes in the network and by implementing a λ-secure property for each of the keys. We concluded that adopting a uniform distribution of the usage of keys in the network can improve the resilience of node-spoofing attacks for other key predistribution schemes.

In addition to the key distribution problems discussed above, our team has developed the following schemes and protocols:

- A network coding scheme for data authenticity and availability in data gathering in multi-hop wireless sensor networks
- A secure multihop broadcasting scheme to provide availability, reliability and authentication for ad-hoc wireless sensor networks
- A protocol for credential based routing in mobile ad-hoc networks in the presence of insider attacks.
- Trust Management and Adversary Detection for delay tolerant sensor networks

In the following paragraphs we summarize the main results from these works as well. Any further details of the schemes can be found in the related publications (listed in the

later part of the report). In all of these publications we have also acknowledged the Army Research Office as the students involving the research were supported in part by the Army Research Office.

In the network coding scheme for data authenticity and availability, we proposed a package of security services for wireless sensor networks in data gathering scenario. The scheme was called location-aware network coding security (LNCS). As the name of the protocol implies, the nodes take advantage of the location information by dividing the terrain into non-overlapping cells and deriving location binding keys during the secure initialization phase. In LNCS, we have eliminated the need to a cluster head, that is responsible for report generation and forwarding in other schemes. This prevents a malicious cluster head from completely compromising the security. In our scheme, an event detected in the field is sensed by several nodes and aggregated by all of them. Using a secret sharing algorithm, the aggregated information is divided into several shares that are forwarded toward the sink in a cell-by-cell fashion. A hash tree based authentication mechanism was utilized to filter out the bogus packets enroute. To provide data availability, we employed random network coding in LNCS. We have provided a comparison between our scheme and previously proposed schemes. The results reveal significant improvement in data availability while maintaining the same level of data confidentiality and authenticity.

Next, we developed a secure multihop broadcasting scheme. Reliability and security of broadcasting is critical in Wireless Sensor Networks (WSNs). Since reliability and security compete for the same resources, we are interested in jointly solving for error control coding (to achieve reliability) and integrity for a broadcast scenario. We assumed Byzantine attacks in which the adversary can compromise nodes and then drop (or modify) the legitimate packets or inject its own packets. For reliable and efficient multihop broadcasting, it is critical to reduce the energy consumption and latency. To prevent the adversary from consuming the scarce network resources by injecting bogus packets, each receiver node should make sure that packets it receives are authentic and it filters out malicious packets immediately. We formed our authentication scheme, on top of a reliable and energy efficient broadcasting protocol called Collaborative Rateless Broadcast (CRBcast) to improve efficiency and reliability. Contrary to the previous schemes, our scheme is resilient with respect to Byzantine adversary as well as routing and flooding attacks and protocol exploits. Moreover, we compared our scheme with the previously proposed broadcast authentication schemes and showed that our scheme outperforms them in terms of efficiency and data availability. This is a crucial improvement over the previous schemes that ensure availability by flooding, introducing very large communication overhead and latency.

In the credential based routing work, we proposed a routing scheme which depends on the trust establishment and a dynamic Bayesian game model between the network nodes. Further, we used rateless codes at the source to avoid retransmissions and to increase data availability. In Mobile Ad-Hoc Networks (MANETs), establishing trust relationships between the nodes in a decentralized fashion has been an important research issue for a long time. If the sender nodes accurately identify the legitimate nodes in the network, a robust

routing can be provided while mitigating the effects of malicious nodes. Further, there is always a mutual interaction between a sender and its neighbor nodes during the communication. This mutual interaction can be easily modeled as a game between two or more players (one player being the sender and the rest being the receivers). Regardless of its type (legitimate or malicious), each player attempts to maximize its benefit during the game by choosing an optimal strategy. We proposed a secure and robust routing scheme in which the interaction between the sender and receiver nodes is modeled using a dynamic Bayesian game model. A repeated game is considered and opinions of a node about the types of other nodes is established using an acknowledgement mechanism from the destination. The proposed method uses the intersection of game theory, trust establishment and coding theory to resist colluding Byzantine (insider) attacks. The scheme guarantees the availability of message as long as a legitimate path exists. Through simulations we showed that the proposed scheme provides low latency and high data availability while keeping the energy consumption moderately low even in highly adversarial environments.

Finally, we will look into the security of delay tolerant sensor networks (DTNs). Specifically, we investigated application of trust and reputation management in such a networks. DTNs are characterized by large end-to-end communication latency and the lack of end-to-end path from a source to its destination. These characteristics pose several challenges to the security of DTNs. Especially, Byzantine attacks in which one or more legitimate nodes have been compromised and fully controlled by the adversary give serious damages to the network in terms of latency and data availability. Using reputation-based trust management systems is shown to be an effective way to handle the adversarial behavior in Mobile Ad-hoc Networks (MANETs). However, because of the unique characteristics of DTNs, those traditional techniques do not apply to DTNs. Our main objective in this work was to develop a robust trust mechanism and an efficient and low cost malicious node detection technique for DTNs. Inspired by our recent results on reputation management for online systems and e-commerce, we developed an iterative malicious node detection mechanism for DTNs referred as ITRM. The iterative reputation management scheme by itself is far more effective than well-known reputation management techniques such as the Averaging Scheme, Bayesian Approach and Cluster Filtering. ITRM is a graph based iterative algorithm motivated by the prior success of message passing techniques for decoding low-density parity-check codes over bipartite graphs. Applying ITRM to DTNs, we observed that the proposed scheme provides high data availability and packet-delivery ratio with low latency in DTNs under adversary attacks.

1.1 Publications and Presentations

While several projects are still ongoing and multiple publications in the near future are expected, the research supported by ARO has resulted in several conference and journal papers as follows (ARO was acknowledged in these publications).

- E. Ayday, F. Delgosha and F. Fekri, "Security Services in Wireless Sensor Networks Using Sparse Random Coding ," in *Proc. the third Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks - IEEE SECON'07*, Reston, VA, 2006.

- E. Ayday, F. Delgosha and F. Fekri, "Location-Aware Security Services for Wireless Sensor Networks Using Network Coding ," in *Proc. IEEE Conference on Computer Communications - INFOCOM'07*, Anchorage, AK, May 2007.

- K. Chan, F. Fekri, Node Compromise Attacks and Secure Connectivity, *SPIE Defense and Security Symposium*, 6758-33, Orlando, Florida USA, April 2007.

- F.Delgosha, E.Ayday, and F. Fekri, "MKPS: A Multivariate Polynomial Scheme for Symmetric Key-Establishment in Distributed Sensor Networks," in *Proc. ACM International Wireless Communications and Mobile Computing Conf. IWCMC'07*, Honolulu, Hawaii, August 2007.

- K.S. Chan, and F. Fekri, "A Resiliency-Connectivity Metric in Wireless Sensor Networks with Key Pre-distribution Schemes and Node Compromise Attacks," *Elsevier Physical Communication*, pp. 134–145, June 2008.

- F. Delgosha, and F. Fekri, "A Multivariate Key-Establishment Scheme for Wireless Sensor Networks," *IEEE Trans. Wireless Communications*, vol. 1, no. 1, March 2008.

- E. Ayday, F. Delgosha, and F. Fekri, "AuCRB: An Efficient Mechanism to Provide Availability, Reliability and Authentication for Multihop Broadcasting in Wireless Networks," *Proc. the Fifth Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks - IEEE SECON'08*, San Francisco, CA, June 2009.

- E. Ayday, and F. Fekri, "Using Node Accountability in Credential Based Routing for Mobile Ad-Hoc Networks," *Proc. of the Fifth IEEE International Conference on Mobile Ad-hoc and Sensor Systems MASS 2008*, (CDROM).

- R. Subramanian, K.S. Chan, and F. Fekri, "Analysis of Latency in Secure Wireless Sensor Networks with Key Pre-distribution," invited paper in 42^{nd} *Asilomar conference on Signals, Systems and Computers,* Pacific Grove, California, Oct. 2008.

- R. Subramanian, and F. Fekri, "Bounds for Lifetime Optimization with Guaranteed Information Delivery in Convergecast Sensor Networks," *Ad Hoc Networks Journal*, accepted with revision June 2009.

- E. Ayday, and F. Fekri, "A Protocol for Data Availability in Mobile Ad-Hoc Networks in the Presence of Insider attacks," *Elsevier Ad Hoc Networks*, accepted, DOI: 10.1016/j.adhoc.2009.07.001, available online http://dx.doi.org/10.1016/j.adhoc.2009.07.001.

- K.S. Chan, F. Fekri, "Resisting Node Spoofing Attacks in Random Key Predistribution Schemes: A Uniform Design," in *2009 IEEE Sarnoff Symposium*, March 2009.
- R. Subramanian and F. Fekri, "Modeling and Analysis of Latency in Distributed Sensor Networks for Converge-cast Traffic," *ACM Transactions on Sensor Networks*, submitted in sept. 2010.
- E. Ayday, H Lee, and F. Fekri, "Trust Management and Adversary Detection for Delay Tolerant Networks," *Proc. Military Communication Conference (MILCOM) 2010*, San Jose, CA, Oct. 2010.
- E. Ayday, F. Delgosha, and F. Fekri, "Data Authenticity and Availability in Multihop Wireless Sensor Networks," *ACM Transactions on Sensor Networks*, accepted Jan. 2010.
- E. Ayday and F. Fekri, "A secure multihop broadcasting scheme to provide availability, reliability and authentication for ad-hoc wireless networks," submitted to *ACM Transactions on Sensor Networks*, submitted Jan. 2010)

1.2 Recognitions and Technology Transitions

- PhD graduate of the team, Kevin Chan, has taken a PostDoc position at United States Army Research Laboratory (ARL), Adelphi, MD in 2008. Now he is a full time employee of US Army Research Lab.
- PhD student of the team, Erman Ayday, took Internship position in QualComm Technology and Samsung in summer 2009 and 2010, respectively, working on security of cellular networks and power grids.
- Ramanan Subramanian (Fekri's Ph.D. student), recipient of the CSIP Outstanding Research Award, 2009. Now he is a Research Fellow at the University of South Australia.
- PhD graduate of the team, F. Delgosha, has taken an Assistant Professor position at New York Institute of technology (NYIT), since 2008.
- E. Ayday, F. Delgosha, and F. Fekri received the Fourth Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (IEEE SECON 2007) best Poster Award.
- F. Fekri received the 2006 Outstanding Junior faculty Award from the School of Electrical and Computer Engineering (Georgia Tech).
- F. Delgosha received the 2006 best Graduate Research Assistant Award from CSIP (the Center for Signal and Image Processing at Georgia Tech).

References

[1] L. Eschenauer and V. Gligor, "A key-management scheme for distributed sensor networks," *ACM Conference on Computer and Communications Security*, 2002.

[2] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," *2003 IEEE Symposium on Security and Privacy*, p. 197, 2003.

[3] R. DiPietro, L. V. Mancini, and A. Mei, "Random key-assignment for secure wireless sensor networks," *Proceedings of the 1st ACM Workshop Security of Ad Hoc and Sensor Networks*, 2003.

[4] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key pre-distribution scheme for wireless sensor networks," *10th ACM Conference on Computer and Communcations Security*, October 2003.

[5] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," *Proceedings for the 10th ACM Conference on Computer and Communication Security*, pp. 52–61, 2003.